Available online at http://www.ijasrd.org/in

International Journal of Advanced Scientific Research & Development

Vol. 03, Iss. 01, Ver. III, Jan – Mar' 2016, pp. 171 – 180

e-ISSN: 2395-6089
p-ISSN: 2394-8906

DETECTION AND PREVENTION OF COLLABORATIVE ATTACKS IN MANET

M. Anusuya[1]
R. Abimaa[1]
M. Abarna[1]

[1] Final Year Students, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

P. Anandraj[2]
N. Murali[2]

[2] Assistant Professor, Department of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India.

ARTICLE INFO

Article History:

Received: 08 Mar 2016;
Received in revised form:
14 Mar 2016;
Accepted: 14 Mar 2016;
Published online: 31 Mar 2016.

Key words:

iTrust Delay Torrent Network (DTN),
Trusted Authority (TA).

ABSTRACT

Malicious and selfish behaviors represent a serious threat against routing in delay/disruption tolerant networks. Due to the unique network characteristics, designing a misbehavior detection scheme in tolerant network (TN) is regarded as a great challenge. The sending information from source to destination, the message stored in a node in spite of destination user in a non- coverage area. In this paper, we propose iTrust Delay Torrent network (DTN), a probabilistic misbehavior detection scheme, for secure DTN several routing toward efficient trust establishment to the base station. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. In this model iTrust as the inspection game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of iTrust DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results demonstrate the effectiveness and efficiency of the proposed scheme.

How to cite this article: Anusuya, M., Abimaa, R., Abarna, M., Anandraj, P., & Murali, N., (2016). "Detection and Prevention of Collaborative Attacks in Manet". *International Journal of Advanced Scientific Research & Development (IJASRD), 03* (01/III), pp. 171 – 180.

INTRODUCTION

DELAY tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information), and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent dis-connectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up). This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion. In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities). Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks.

The recent researches show that routing misbehavior will significantly reduce the packet delivery rate and, thus, pose a serious threat against the network performance of DTN. Therefore, a misbehavior detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the secured among DTN nodes in DTNs. Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks. These works use neighborhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes. Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficulty to predict mobility patterns, and long feedback delay have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs. Selfish node B receives the packets from node A but launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior (e.g., dropping messages) cannot be detected due to lack of witness, which renders the monitoring-based misbehavior detection less.

EXISTING SYSTEM

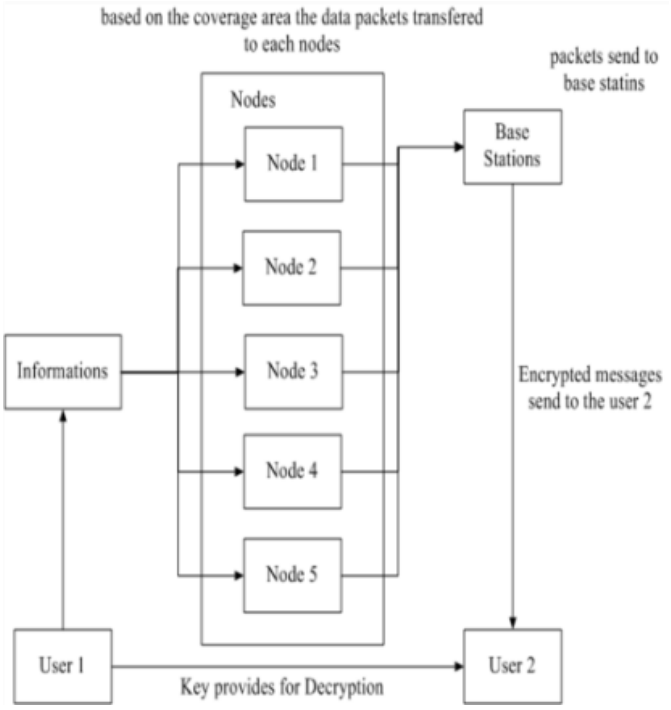
In this existing system the individual user data can be exchanged over the thirds party server. Individual data can be accessed through the third party server, and it can be out sourced. Before outsourcing, the secrecy data to be encrypt and outsource the data. In this system, the particular secrecy data can be maintained by the central authority (CA) to the key management on behalf of third party owners. In this system, the malicious behaviors which may lead to the exposure of the secrecy data. In Existing the access policy based mechanism is not used. The nodes are trusted blindly.

PROPOSED SYSTEM

In the proposed system, iTrust Delay Torrent Network (DTN) is preferred for the Packets Node transmission and the secure sharing of secrecy data is storing on the trusted base station server storage nodes in presence of key management by users. It can be protected using the CP-ABE (Cipher text-Policy Attribute-Based Encryption) can be used to encrypt the particular user data as per the user needs. The encryption and the decryption of the key generation can be based on the type of attributes that user chooses depend on the key authorities. In this to improve security the user is categorized into public access data and the personal domains can be categorized. In the public domain, we will use multi authority to improve the security and to avoid unauthorized user access problem. Probabilistic Value is Calculated for Every nodes to identify node Trust.

SYSTEM ARCHITECTURE

Fig. 1: *Architecture Diagram*



ALGORITHM ANALYSIS

DES (the Data Encryption Standard) is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1.

The algorithm is best suited to implementation in hardware, probably to discourage implementations in software, which tend to be slow by comparison. However, modern computers are so fast that satisfactory software implementations are readily available.

DES is the most widely used symmetric algorithm in the world, despite claims that the key length is too short. Ever since DES was first announced, controversy has raged about whether 56 bits is long enough to guarantee security.

The key length argument goes like this. Assuming that the only feasible attack on DES is to try each key in turn until the right one is found, then 1,000,000 machines each capable of testing 1,000,000 keys per second would find (on average) one key every 12 hours. Most reasonable people might find this rather comforting and a good measure of the strength of the algorithm.

Those who consider the exhaustive key-search attack to be a real possibility (and to be fair the technology to do such a search is becoming a reality) can overcome the problem by using double or triple length keys. In fact, double length keys have been recommended for the financial industry for many years.

Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:

- Encrypt with K1
- Decrypt with K2
- Encrypt with K3

Decryption is the reverse process:

- Decrypt with K3
- Encrypt with K2
- Decrypt with K1

Setting K3 equal to K1 in these processes gives us a double length key K1, K2.

Setting K1, K2 and K3 all equal to K has the same effect as using a single-length (56-bit key). Thus it is possible for a system using triple-DES to be compatible with a system using single-DES.

Pseudocode

```
Cipher (plainBlock[64], RoundKeys[16, 48], cipherBlock[64])
{
 permute (64, 64, plainBlock, inBlock, InitialPermutationTable)
 split (64, 32, inBlock, leftBlock, rightBlock)
 for (round = 1 to 16)
 {
 mixer (leftBlock, rightBlock, RoundKeys[round])
 if (round!=16) swapper (leftBlock, rightBlock)
 }
 combine (32, 64, leftBlock, rightBlock, outBlock)
 permute (64, 64, outBlock, cipherBlock, FinalPermutationTable)
}
mixer (leftBlock[48], rightBlock[48], RoundKey[48])
{
 copy (32, rightBlock, T1)
 function (T1, RoundKey, T2)
 exclusiveOr (32, leftBlock, T2, T3)
 copy (32, T3, rightBlock)
```

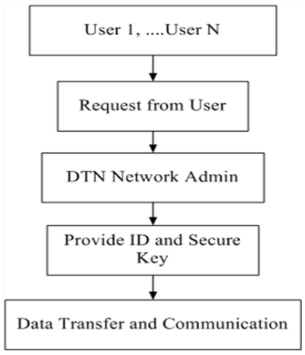
```
  }
  swapper (leftBlock[32], rigthBlock[32])
  {
   copy (32, leftBlock, T)
   copy (32, rightBlock, leftBlock)
   copy (32, T, rightBlock)
  }
  function (inBlock[32], RoundKey[48], outBlock[32])
  {
   permute (32, 48, inBlock, T1, ExpansionPermutationTable)
   exclusiveOr (48, T1, RoundKey, T2)
   substitute (T2, T3, SubstituteTables)
   permute (32, 32, T3, outBlock, StraightPermutationTable)
  }
  substitute (inBlock[32], outBlock[48], SubstitutionTables[8, 4, 16])
  {
   for (i = 1 to 8)
   {
 row ¨ 2 ¥ inBlock[i ¥ 6 + 1] + inBlock [i ¥ 6 + 6]
 col ¨ 8 ¥ inBlock[i ¥ 6 + 2] + 4 ¥ inBlock[i ¥ 6 + 3] +
 2 ¥ inBlock[i ¥ 6 + 4] + inBlock[i ¥ 6 + 5]
 value = SubstitutionTables [i][row][col]
 outBlock[[i ¥ 4 + 1] ¨ value / 8; value ¨ value mod 8
 outBlock[[i ¥ 4 + 2] ¨ value / 4; value ¨ value mod 4
 outBlock[[i ¥ 4 + 3] ¨ value / 2; value ¨ value mod 2
 outBlock[[i ¥ 4 + 4] ¨ value
 }
}
```

MODULES

1. DTN Network Initialization
2. Identify Possible Path from Source to Destination
3. Secure Data Transfer by using DES
4. Identify the Coverage and Non-Coverage Node for packets transmission

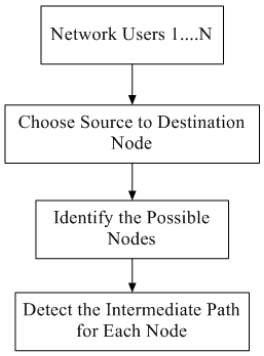
DTN Network Initialization: The DTN network is used for data transfer in Military Applications, due to the Storage Capacity and Coverage type. The DTN network is constructed to the Military Users for Communication to the group of users based on the Coverage range. The User requested to the DTN network is joined to the network by the network provider Admin. Network formation based on the node formation of the area and Each Node is provided with Network Id and Secure Key for Data Transfer and Communication.

Fig. 2: *DTN Network Initialization*



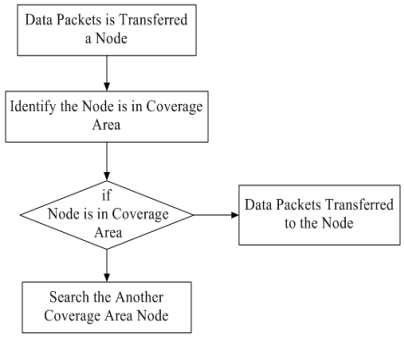
Identify Possible Path from Source to Destination: In DTN network, the users to communicate with each other, the network users should be within the communicate range interconnected with multi number of nodes. The Network User is not to be aware of each node and make request to the base station, and the data send through number of packets in each node, if the connection is establish to the destination user, then the number of possible node path is to be identify from Source node to the base station. Then for each path the Intermediate node is to be Determined.

Fig. 3: *Identifying Possible Path*



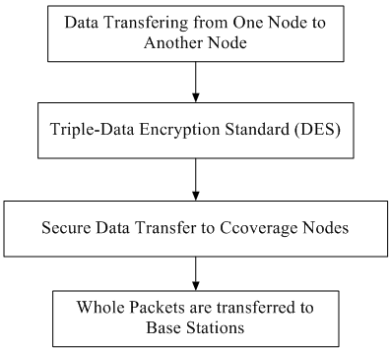
Identify the Coverage and Non-Coverage Node for packets transmission: The DTN node is monitored by each node in the tolerant networks. The Data packets is transferred to nearest node. DTN search the nearest coverage nodes. If the node is in coverage area, the data packets transferred. Otherwise the DTN search the another coverage node, For Example consider 3 nodes A, B, C So it distributes a broadcast message to each node A and C enquiring B, If the node A and B relays the Data Transfer Information and Acknowledgement of B, Then the data is transferred to B node is in coverage area, otherwise the packets transferred to node c.

Fig. 4: *Identifying Node for Packet Transmission*

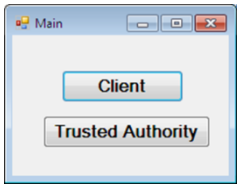


Secure Data Transfer by using DES: The node is transferred based on the Delay Torrent Network, and the Node Security is determined, Now to improve the monitoring of the Data in the coverage area, Triple-Data Encryption Standard (DES) is Used, triple DES means data Encryption it Encrypts the node packets, then the Cipher text is transferred through the each node, The protocol agents thus act as surrogates for end-to-end sources and destinations, then the Cipher text is received and decrypted by the Destination node by Efficient Key Management.

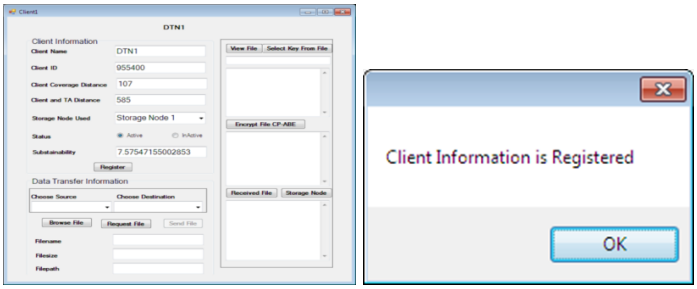
Fig. 5: *Using DES*



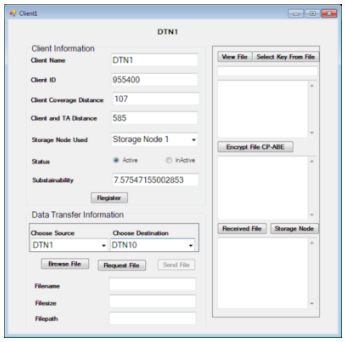
EXPERIMENTAL RESULT



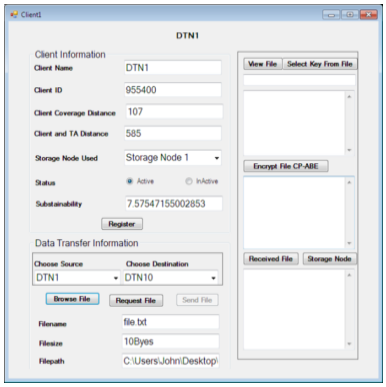
(i) Registration for Client



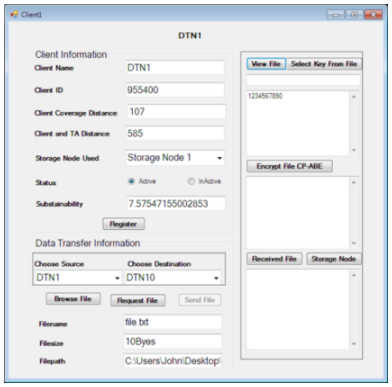
(ii) Data Transfer Information of Source to Destination



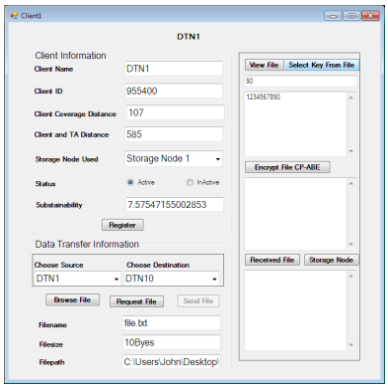
(iii) Information of Selected File



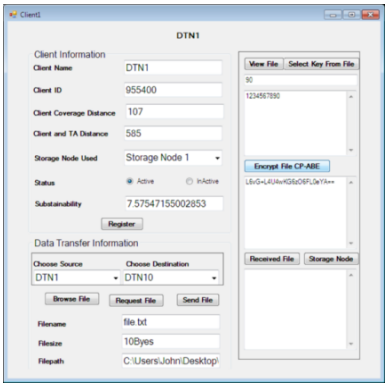
(iv) View the Selected file



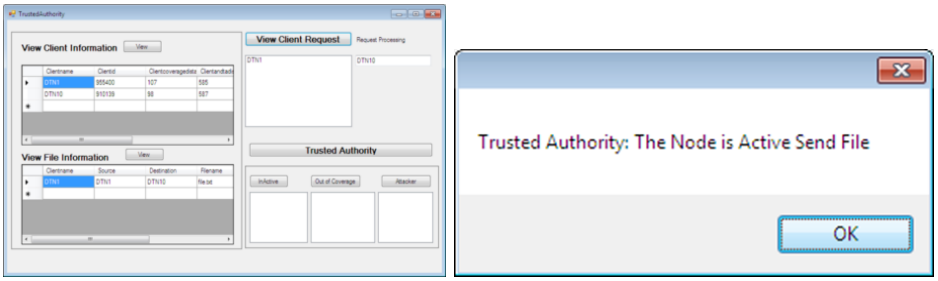
(v) Select Key from a File



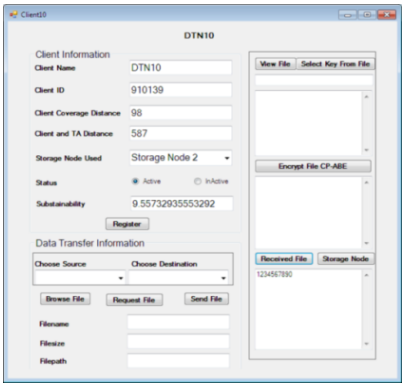
(vi) Using CP-ABE on Select Key from File



(vii) View Client Request Information



(viii) Receive File to Authorized Destination User



CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. DES is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using DES for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

FUTURE ENHANCEMENT

In DES the idea is purely related on the security of data, No one is concentrated on the problem in data transmission, to avoid such thread, the nodes in the DTN network are monitored by Trusted Authority and set a probabilistic value, the probabilistic value denotes the node trust. So the Probabilistic misbehavior Scheme is used for secure data transmission.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp: Routing for vehicle-based disruption-tolerant networking," in Proc. IEEE Conf. Comput. Commun, Barcelona, Spain, Apr. 2006, pp. 1–11.

[2] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket switched networks and the consequences of human mobility in conference environments," in Proc. ACM SIGCOMM Workshop Delay Tolerant Netw., Philadelphia, PA, USA, Aug. 2005, pp. 244–251.

[3] D. Zhao, H. Ma, S. Tang, et al., "COUPON: A cooperative framework for building sensing maps in mobile opportunistic networks," to appear in IEEE Trans. Parallel Distrib. Syst., Feb.2014.

[4] A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, "Low-cost communication for rural internet kiosks using mechanical backhaul," in Proc. 12th Annu. ACM Int. Conf. Mobile Comput. Netw., Los Angeles, CA, USA, Sep. 2006, pp. 334–345

[5] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," IEEE/ACM Trans. Netw., vol. 10, no. 4, pp. 477–486, Aug. 2002.

[6] P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 388–404, Mar. 2000.

[7] P. Li, Y. Fang, J. Li, and X. Huang, "Smooth trade-offs between throughput and delay in mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 11, no. 3, pp. 427–438, Mar. 2012.

[8] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, and Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE Transactions on Parallel and Distributed Systems, 25 (1), pp. 22 – 32, Jan 2014.

[9] S. P. Vijayaragavan, E. Vadivel, and M. Sriram, "Efficient Trust Establishment in Delay - Tolerant Networks Based on iTrust Protocol", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 4 (6), pp. 5323 – 5328, June 2015, doi: 10.15662/ijareeie.2015.0406181.

[10] D. Kerana Hanirex and Pritiviraj. V, "An iTrust Based Misbehaviour Detection Technique on Clustered Nodes in Delay Tolerant Network", Journal Research in Electrical Electronics and Communications, pp. 1 – 9, March Issue 2015.

[11] Vigneshkumar. P., and Senthilnathan. K. R., "A Survey on Trust Establishment in Delay Tolerant Networks", International Journal of Computer Science and Mobile Computing, 3 (11), pp. 548 – 554, November 2014.

[12] The Cryptography Guide: Triple DES, Retrieved from http://www.cryptographyworld.com/des.htm.